ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 128 (2008) 662–679

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Parity of ranks for elliptic curves with a cyclic isogeny

Tim Dokchitser [a,*], Vladimir Dokchitser [b]

[a] *Robinson College, Cambridge CB3 9AN, United Kingdom*
[b] *Max Planck Institut für Mathematik, D-53111 Bonn, Germany*

Received 3 August 2006; revised 21 February 2007

Available online 16 May 2007

Communicated by David Goss

Abstract

Let E be an elliptic curve over a number field K which admits a cyclic p-isogeny with $p \geqslant 3$ and semistable at primes above p. We determine the root number and the parity of the p-Selmer rank for E/K, in particular confirming the parity conjecture for such curves. We prove the analogous results for $p = 2$ under the additional assumption that E is not supersingular at primes above 2.

Keywords: Parity conjecture; Elliptic curves; Selmer rank; Root numbers

1. Introduction

If E is an elliptic curve over a number field K, the number of copies of $\mathbb{Z}$ in the group of rational points $E(K)$ is called the Mordell–Weil rank of E/K. If the Tate–Shafarevich group $Ш(E/K)$ is finite (conjecturally, this is always the case), then for every prime p it is the same as the p-Selmer rank of E/K, defined as the Mordell–Weil rank plus the number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ in $Ш(E/K)$. We will be concerned with the parity of the p-Selmer rank, and we will write $\sigma(E/K, p)$ for $(-1)^{p\text{-Selmer rank of } E/K}$.

Tate's generalization of the Birch and Swinnerton–Dyer conjecture for elliptic curves over number fields predicts that the Mordell–Weil rank is the same as the analytic rank, the order of vanishing of the L-function $L(E/K, s)$ at $s = 1$. The parity of the analytic rank is determined

* Corresponding author.
E-mail addresses: t.dokchitser@dpmms.cam.ac.uk (T. Dokchitser), v.dokchitser@dpmms.cam.ac.uk (V. Dokchitser).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.02.008

by the root number $w(E/K) \in \{\pm 1\}$, which is the conjectural sign in the functional equation for $L(E/K, s)$ under $s \leftrightarrow 2 - s$. Although this L-function is not even known to exist at $s = 1$ for $K \neq \mathbb{Q}$, the definition of the root number (due to Langlands) is independent of any conjectures. Thus we expect the following parity conjecture:

Conjecture 1. *For any (some) prime p, the root number agrees with the parity of the p-Selmer rank, so $w(E/K) = \sigma(E/K, p)$.*

One of the main results in the paper is the following theorem.

Theorem 2. *If E/K has a rational isogeny of prime degree $p \geqslant 3$, and E is semistable at all primes over p, then Conjecture 1 holds for E/K and p. It also holds for $p = 2$ under the additional assumption that E is not supersingular at primes above 2.*

Recall that the global root number can be expressed in terms of local root numbers over all places of K,

$$w(E/K) = \prod_v w(E/K_v).$$

If E has an isogeny ϕ of degree p over K, then there is also a product formula for the parity of the p-Selmer rank (Cassels–Fisher, see [1, Appendix]),

$$\sigma(E/K, p) = \prod_v \sigma_\phi(E/K_v).$$

Here $\sigma_\phi(E/K_v) \in \{\pm 1\}$ is 1 if the power of p in

$$\frac{\#\operatorname{coker}(\phi : E(K_v) \to E'(K_v))}{\#\ker(\phi : E(K_v) \to E'(K_v))}$$

is even and -1 otherwise.

Notation. If F is a local field, we write $(a, b) = (a, b)_F \in \{\pm 1\}$ for the Hilbert symbol: it is 1 if and only if b is a norm from $F(\sqrt{a})$ to F.

If $\phi : E \to E'$ is an isogeny defined over F, we write F_ϕ for the extension of F generated by the points in $\ker\phi$. Since $\mathrm{Gal}(F_\phi/F) \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^*$ from the action on these points, F_ϕ/F is cyclic. We denote the image of -1 under the composition

$$F^* \xrightarrow{\text{loc.recip.}} \mathrm{Gal}(F_\phi/F) \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^*$$

by $(-1, F_\phi/F)$, and we refer to it as the local Artin symbol. It is 1 if -1 is a norm from F_ϕ to F and -1 otherwise.

In this paper we derive formulae for the local terms $w(E/K_v)$ and $\sigma_\phi(E/K_v)$ for odd p (Theorems 5 and 6). It turns out that although the root number and the p-Selmer rank agree globally, the local terms are not the same but are related as follows.

Theorem 3. *Let K be a number field and p an odd prime. Let E/K be an elliptic curve with a cyclic p-isogeny ϕ defined over K, and assume that E has semistable reduction at all primes above p. Then for all places v of K,*

$$w(E/K_v) = (-1, K_{v,\phi}/K_v)\sigma_\phi(E/K_v).$$

Note that Theorem 3 implies Theorem 2 by the product formula for the local Artin symbols, $\prod_v (-1, K_{v,\phi}/K_v) = 1$.

When $p = 2$, the above theorem does not hold. The existence of a 2-isogeny is equivalent to having a 2-torsion point, so the extension $K_{v,\phi}/K_v$ is always trivial. However, there is an analogous relation between $w(E/K_v)$ and $\sigma_\phi(E/K_v)$ as follows.

Translating the 2-torsion point to $(0, 0)$, the curves E and E' get the models

$$E\colon \quad y^2 = x^3 + ax^2 + bx, \qquad a, b \in \mathcal{O}_K, \tag{1}$$

$$E'\colon \quad y^2 = x^3 - 2ax^2 + \delta x, \qquad \delta = a^2 - 4b, \tag{2}$$

with the isogeny $\phi : E \to E'$ given by

$$\phi : (x, y) \mapsto \bigl(x + a + bx^{-1}, y - bx^{-2}y\bigr). \tag{3}$$

Theorem 4. *Suppose E/K has either good ordinary or multiplicative reduction at all primes above 2. Then for all places v of K,*

$$w(E/K_v) = \sigma_\phi(E/K_v)(a, -b)_{K_v}(-2a, \delta)_{K_v}. \tag{4}$$

In particular, the 2-parity conjecture holds for E/K by the product formula for the Hilbert symbols.

For $K = \mathbb{Q}$, the parity conjecture for E and p in the case that E has a p-isogeny is a theorem of P. Monsky [6], who also proved it unconditionally for $K = \mathbb{Q}$, $p = 2$. J. Nekovář [7] proved the conjecture without the assumption on the existence of a p-isogeny for elliptic curves over $\mathbb{Q}$ with potentially ordinary or potentially multiplicative reduction at p. If $E/\mathbb{Q}$ is semistable and has a rational p-isogeny (p odd), the parity conjecture for E base changed to an arbitrary number field follows from [1, Thm. 3 and Prop A.1]. Indeed, our computations of Selmer ranks are based on the approach by T. Fisher in [1]. We would also like to mention that for $E/\mathbb{Q}$, recently M. Shuter [12] has done some beautiful computations of Selmer ranks over the fields where they acquire a p-isogeny.

2. Main results for $p \geqslant 3$

Theorem 5. *Assume $F = \mathbb{R}$ or $\mathbb{C}$, or $[F : \mathbb{Q}_l] < \infty$, and let $p \geqslant 3$. Let E/F be an elliptic curve with a rational p-isogeny ϕ. Then*

$$w(E/F) = \begin{cases} -1 & F \text{ is Archimedean}, \\ 1, & E \text{ has good reduction}, \\ -1, & E \text{ has split multiplicative reduction}, \\ 1, & E \text{ has non-split multiplicative reduction}, \\ \delta \cdot (-1, F_\phi/F), & E \text{ has additive reduction and } l \neq p. \end{cases}$$

Here $\delta = 1$ unless $p = 3$, $\mu_3 \not\subset F$ and E/F has reduction type IV *or* IV*, *in which case $\delta = -1$.*

Proof. Except in the case of additive reduction, the formula for $w(E/F)$ is well known and does not depend on the existence of a rational isogeny (see e.g. [9, Thm. 2]). The remaining case is dealt with in Section 3. □

Theorem 6. *Assume $F = \mathbb{R}$ or $\mathbb{C}$, or $[F : \mathbb{Q}_l] < \infty$, and let $p \geqslant 3$. Let E/F be an elliptic curve with a rational p-isogeny ϕ. Then*

$$\sigma_\phi(E/F) = \begin{cases} -(-1, F_\phi/F), & F \text{ is Archimedean}, \\ (-1, F_\phi/F), & E \text{ has good reduction}, \\ -(-1, F_\phi/F), & E \text{ has split multiplicative reduction}, \\ (-1, F_\phi/F), & E \text{ has non-split multiplicative reduction}, \\ \delta, & E \text{ has additive reduction and } l \neq p. \end{cases}$$

Here $\delta = 1$ unless $p = 3$, $\mu_3 \not\subset F$ and E/F has reduction type IV *or* IV*, *in which case $\delta = -1$.*

Remark on Artin symbols. For $l \neq p$ the above local Artin symbols can be easily described: If F is Archimedean, $(-1, F_\phi/F) = 1$ (i.e. -1 is a norm from F_ϕ) unless $F = \mathbb{R}$ and $F_\phi = \mathbb{C}$. If F is non-Archimedean and E has semistable reduction, then $(-1, F_\phi/F) = 1$ because this extension is unramified (see proof below). For $l = p$, see Lemma 12 for the description of the Artin symbol.

Proof of Theorem 6. Recall that $\sigma_\phi(E/F) = \pm 1$ and it is 1 if and only if the power of p in

$$\frac{\#\mathrm{coker}(\phi : E(F) \to E'(F))}{\#\ker(\phi : E(F) \to E'(F))} \tag{5}$$

is even. For Archimedean F, the cokernel is always trivial while $\#\ker = p$ unless $F = \mathbb{R}$ and $F_\phi = \mathbb{C}$; so $\sigma_\phi(E/F) = -(-1, F_\phi/F)$.

Henceforth assume that F is a finite extension of $\mathbb{Q}_l$. Then (5) equals [1, App., formula (18)]

$$\frac{c_v(E')}{c_v(E)} \cdot |\alpha_v|_v^{-1}$$

where c_v is the Tamagawa number and α_v is the leading coefficient for the action of ϕ on the formal groups. We will compute both contributions.

For the quotient $c_v(E')/c_v(E)$, Lemma 11 in Section 4 shows that it has odd p-valuation precisely for the primes of split multiplicative reduction and primes of additive reduction with $\delta = -1$. Next, for $l \nmid p$, the isogeny ϕ induces an isomorphism on formal groups, so α_v is a unit. For $l|p$, we will show that $\mathrm{ord}_p |\alpha_v|_v$ is even if and only if $(-1, F_\phi/F) = 1$ (Section 6).

To complete the proof of the theorem, it remains to show that $(-1, F_\phi/F) = 1$ for places $l \nmid p$ of semistable reduction. It suffices to check that F_ϕ/F is unramified, since then all units are norms by local class field theory. But F_ϕ/F is a Galois extension of degree prime to p, while the inertia subgroup of $\mathrm{Gal}(K_v(E[p])/K_v)$ is either trivial in case of good reduction or a p-group in case of multiplicative reduction (cf. [14, Exc. 5.13]). $\square$

Corollary 7. *Let K be a number field and E/K an elliptic curve with semistable reduction at all primes above p. Assume E has a rational p-isogeny ϕ. Then*

$$w(E/K) = \sigma(E/K, p) = (-1)^{\#\{v|\infty\}}(-1)^s \prod_{v \text{ additive}} \delta_v(-1, K_{v,\phi}/K_v),$$

where s is the number of primes of split multiplicative reduction of E/K, and $\delta_v = 1$ unless $p = 3$, $\mu_3 \not\subset K_v$ and E has reduction type IV *or* IV* *at v, in which case $\delta_v = -1$.*

Since the local Artin symbol over the semistable primes $v \nmid p$ is trivial, it follows from the product formula that the product over the additive primes can be replaced by the ones over p and over ∞, apart from the easy correction terms δ_v (trivial for $p > 3$),

$$w(E/K) = \sigma(E/K, p) = (-1)^{\#\{v|\infty\}}(-1)^s \prod_{v|p \text{ or } \infty} (-1, K_{v,\phi}/K_v) \prod_{v \text{ additive}} \delta_v.$$

3. Root numbers

In this section $[F : \mathbb{Q}_l] < \infty$ and E/F is an elliptic curve with additive reduction which admits a cyclic p-isogeny for some odd $p \neq l$. To complete the proof of Theorem 5 we need to show that

$$w(E/F) = \delta \cdot (-1, F_\phi/F),$$

where $\delta = 1$ unless $p = 3$, $\mu_3 \not\subset F$ and E/F has reduction type IV or IV*, in which case $\delta = -1$. Recall also that F_ϕ is the extension of F generated by the points in the kernel of ϕ.

We will determine $w(E/F)$ from the action of $\mathrm{Gal}(\bar{F}/F)$ on the p-adic Tate module $T_p(E)$. We mention that computations of this kind have previously been carried out by Rohrlich [8,9] and Kobayashi [3], and we refer to them for definitions and background for local root numbers and ϵ-factors of elliptic curves.

We set $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$, and recall that the Weil group of F is the subgroup of $\mathrm{Gal}(\bar{F}/F)$ generated by the inertia subgroup and a lifting Frob of the Frobenius element. Write $\|\cdot\|$ for the cyclotomic character (local reciprocity map composed with the normalized absolute value of F).

Lemma 8. *Suppose E has potentially multiplicative reduction. Then the action of the Weil group on $V_p(E)$ is of the form $\left(\begin{smallmatrix}\chi & * \\ 0 & \chi^{-1}\|\cdot\|\end{smallmatrix}\right)$ for some ramified quasi-character χ, and inertia acts via $\pm\left(\begin{smallmatrix}1 & * \\ 0 & 1\end{smallmatrix}\right)$ with $*$ not identically 0. The root number is given by $w(E/F) = (-1, F_\phi/F)$.*

Proof. That inertia acts as asserted follows the theory of the Tate curve (cf. [14, Lemma V.5.2, Excs. 5.11, 5.13]). In particular, E acquires multiplicative reduction over F_ϕ.

Because the inertia subgroup is normal in the Weil group, Frobenius preserves the 1-dimensional subspace where inertia acts through a quotient of order 2; this gives the action of the full Weil group.

Next, the root number of the semi-simplification of $V_p(E)$ is given by the determinant formula (see [8, p. 145] or [15, (3.4.7)])

$$w\big(V_p(E)_{ss}\big) = w\big(\chi \oplus \chi^{-1}\| \cdot \|\big) = w\big(\chi \oplus \chi^{-1}\big) = \chi\big(\theta(-1)\big)$$

with θ the local reciprocity map on F^*. Over F_ϕ the quasi-character χ, and therefore also $V_p(E)_{ss}$, is unramified. Take a primitive character $\tilde{\chi}$ of F_ϕ/F that coincides with χ on inertia. Then

$$\chi\big(\theta(-1)\big) = \tilde{\chi}\big(\theta(-1)\big) = (-1, F_\phi/F).$$

The assertion follows from the formula (see [15, (4.2.4)])

$$\epsilon\big(V_p(E)\big) = \epsilon\big(V_p(E)_{ss}\big)\frac{\det(-\operatorname{Frob}^{-1} \mid V_p(E)_{ss}{}^I)}{\det(-\operatorname{Frob}^{-1} \mid V_p(E)^I)}, \tag{6}$$

since $V_p(E)_{ss}{}^I = 0 = V_p(E)^I$. $\square$

Lemma 9. *Suppose E has potentially good reduction and $p \geqslant 5$. Then the action of the Weil group on $V_p(E)$ is of the form $\left(\begin{smallmatrix}\chi & 0 \\ 0 & \chi^{-1}\|\cdot\|\end{smallmatrix}\right)$ for some quasi-character χ. The root number is given by $w(E/F) = (-1, F_\phi/F)$.*

Proof. From the properties of the Weil pairing, inertia acts via $\left(\begin{smallmatrix}1 & * \\ 0 & 1\end{smallmatrix}\right)$ on $E[p]$ over F_ϕ. On the other hand, the inertia is finite of order dividing 24 [10, §5.6], so has no elements of order p. So it acts trivially on $E[p]$, hence E/F_ϕ has good reduction (by [11, Cor. 2] or [14, Prop 10.3]).

We need to show that the action of the Weil group on $V_p(E)$ is abelian. On the one hand, the commutator of any two elements acts trivially on the residue field, so it is an element of the inertia subgroup. On the other hand, its image in $\operatorname{Gal}(F_\phi/F)$ is trivial, because the latter is abelian. As E/F_ϕ has good reduction, this commutator acts trivially on $T_p(E)$.

It follows that $T_p(E) \cong \chi \oplus \chi^{-1}\| \cdot \|$, so $w(E/F) = (-1, F_\phi/F)$ as in the proof of Lemma 8. $\square$

Lemma 10. *Suppose E has potentially good reduction and $p = 3$. Then $w(E/F) = \delta(-1, F_\phi/F)$.*

Proof. Denote $G = \operatorname{Gal}(F(E[3])/F)$ and write I for its inertia subgroup. Since I is a non-trivial subgroup of $\left(\begin{smallmatrix}* & * \\ 0 & *\end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_3)$ of determinant 1, it is one of C_2, C_3 and C_6. Moreover, $I = C_3$ if and only if E has reduction type IV or IV*. (For $l \neq 2$, E has type IV or IV* if and only if the valuation of the minimal discriminant of E is 4 or 8, equivalently $|I|=3$. For $l=2$, see [5, Thm. 2(i)].)

(a) If $I=C_2$, then $\delta=1$. The root number is $(-1,F_\phi/F)$ by the same argument as in Lemma 9.

(b) If $I=C_3$, then $(-1,F_\phi/F)=1$ because it corresponds to an element of I of order dividing 2. Next, G is either C_3 or C_6 if $\mu_3\subset F$, and S_3 otherwise.

If G is cyclic, then $w(E/F)=1$, because E acquires good reduction after a Galois cubic extension, and the root number of an elliptic curve is unchanged in such an extension [4, proof of Prop. 3.4].

If $G=S_3$, then Frob^2 acts centrally on $V_3(E)$, so it is given by a scalar matrix $\lambda\,\mathrm{Id}$. From the properties of the Weil pairing, its determinant λ^2 is equal to $\det(\mathrm{Frob})^2=f^2$, where f is the size of the residue field of F. Note that $f\equiv 2 \bmod 3$ as $\mu_3\not\subset F$ and $\lambda\equiv 1 \bmod 3$ since Frob^2 acts trivially on $E[3]$. In other words $\lambda=-f$.

Let χ be the unramified quasi-character of the Weil group that takes Frobenius to $1/\sqrt{-f}\in\mathbb{Q}_3$. Then $V_3(E)\otimes\chi$ coincides with the 2-dimensional irreducible representation of $G\cong S_3$. If ϕ is a character of order 3 of I, then by a theorem of Fröhlich–Queyrut [2, Lemma 1 and Thm. 3],

$$w(\phi)=\phi\bigl(\theta\bigl(\sqrt{-3}\bigr)\bigr)=1,$$

where θ is the local reciprocity map on $F(\mu_3)^*$.

Let η be the quadratic unramified character of G, and denote by m the largest integer such that $\mathrm{tr}_{F/\mathbb{Q}_l}(\pi_F^{-m}\mathcal{O}_F)\subset\mathbb{Z}_l$. Writing $\mathbf{1}$ for the trivial representation, by inductivity in degree 0,

$$1=\frac{w(\phi)}{w(\mathbf{1}_{F(\mu_3)})}=\frac{w(V_3(E)\otimes\chi)}{w(\mathbf{1}_F)w(\eta)}=\frac{w(V_3(E)\otimes\chi)}{\eta(\mathrm{Frob})^m}=(-1)^m w\bigl(V_3(E)\otimes\chi\bigr).$$

On the other hand, by the tensor product formula [15, (3.4.6)],

$$\epsilon\bigl(V_3(E)\otimes\chi\bigr)=\chi\bigl(\mathrm{Frob}^{-1}\bigr)^{n(E)+2m}\epsilon\bigl(V_3(E)\bigr),$$

so $w(E/F)=(-1)^{n(E)/2}=-1$ because $n(E)=2$ (tame ramification).

(c) Now assume that $I=C_6$. Then $G=C_6$ if $\mu_3\subset F$ and $G\cong D_{12}$ otherwise. In the first case, the action of the Weil group is abelian, so the same argument as in Lemma 9 applies, and $w(E/F)=(-1,F_\phi/F)$.

Finally, suppose $G\cong D_{12}$ and consider the twist E_χ of E by the non-trivial character χ of the quadratic extension F_ϕ/F. By inductivity in degree 0,

$$\frac{w(E/F_\phi)}{w(\mathbf{1}_{F_\phi}\oplus\mathbf{1}_{F_\phi})}=\frac{w(E/F)w(E_\chi/F)}{w(\mathbf{1}_F)^2w(\chi)^2}.$$

Both E/F_ϕ and E_χ/F have root number -1, as they fall under case (b) with $G=S_3$. By the determinant formula,

$$w(E/F)=w(\chi)^2=w\bigl(\chi\oplus\chi^{-1}\bigr)=\det(\chi)(-1)=(-1,F_\phi/F).\qquad\square$$

4. Tamagawa numbers

In the next three sections, we complete the proof of Theorem 6.

Lemma 11. *Let E/F be an elliptic curve, $[F:\mathbb{Q}_l]<\infty$. Suppose $\phi: E\to E'$ is a cyclic p-isogeny defined over F with $p\geqslant 3$. Denote by $c(E)=[E(F):E_0(F)]$, $c(E')=[E'(F):E'_0(F)]$ the Tamagawa numbers, and let δ be as in Theorems 5 and 6. Then*

$$\operatorname{ord}_p \frac{c(E')}{c(E)} = \begin{cases} 0, & E \text{ has good or non-split multiplicative reduction},\\ \pm 1, & E \text{ has split multiplicative reduction},\\ 0, & E \text{ has additive reduction and } \delta = 1,\\ \pm 1, & E \text{ has additive reduction and } \delta = -1. \end{cases}$$

Proof. If E (and therefore also E') has good reduction, then $c(E)=c(E')=1$. If E has non-split multiplicative reduction, then the c are 1 or 2, so the quotient is prime to p. If the reduction is split multiplicative, the quotient contributes either p or p^{-1} [1, Lemma A.2]. If E has additive reduction then $1\leqslant c\leqslant 4$, so the quotient is prime to p for $p\geqslant 5$. It suffices to prove that for $p=3$ the quotient is prime to 3 precisely when $\delta=1$.

From Tate's algorithm [14, IV.9], the case $c=3$ only occurs when the reduction type is IV or IV*. Applying the multiplication-by-3 map to the exact sequence

$$0 \longrightarrow E_0(F) \longrightarrow E(F) \longrightarrow E(F)/E_0(F) \longrightarrow 0$$

and recalling that it is an isomorphism on formal groups, we get that $E(F)$ has a 3-torsion point if and only if $c=3$.

If the absolute Galois group acts on $E[3]$ via $\left(\begin{smallmatrix}\chi_1 & *\\ 0 & \chi_2\end{smallmatrix}\right)$, then its action on $E'[3]$ is of the form $\left(\begin{smallmatrix}\chi_1 & 0\\ * & \chi_2\end{smallmatrix}\right)$. Also note that $\mu_3\subset F$ if and only if the action factors through $\mathrm{SL}_2(\mathbb{F}_3)$. So if $\mu_3\subset F$, then $E(F)$ has a 3-torsion point if and only if the isogenous curve has one, so $c(E)/c(E')=1$. Conversely, if $\mu_3\not\subset F$, exactly one of $E(F), E'(F)$ has a 3-torsion point, so $c(E)/c(E')=3^{\pm 1}$. $\square$

5. Local Artin symbols at primes above *p*

Lemma 12. *Let $\mathbb{Q}_p\subset F\subset F'$ be finite extensions (p odd), with F'/F cyclic Galois of degree dividing $p-1$. Then $(-1, F'/F)=1$ if and only if one of the following conditions is satisfied:*

(1) *The residue field k_F of F is of even degree over $\mathbb{F}_p$, or*
(2) *$(p-1)/e(F'/F)$ is even, where e denotes ramification degree.*

Proof. The condition $(-1, F'/F)=1$ is equivalent to -1 being a norm from F' to F. If F_0 is the maximal odd degree extension of F inside F', then $N_{F_0/F}(-1)=-1$, implies $(-1,F'/F)=(-1,F'/F_0)$. In other words, we may assume that $[F':F]$ is a power of 2.

Let F^u be the maximal unramified extension of F inside F'. If $F^u=F'$, then all units of F are norms from F' and the result holds. Otherwise, we can write $-1=\zeta^{[F^u:F]}=N_{F^u/F}(\zeta)$ for some $\zeta\in\mu_{p-1}\subset F$. Then $(-1,F'/F)=1$ if and only if ζ is a norm from F' to F^u.

Since F'/F^u is a totally and tamely ramified extension, a unit in F^u is a norm from F' if and only if its reduction lies in the unique subgroup of k^* of index $[F':F^u]$, where k is the residue field of F^u.

Writing $d=[F^u:F]$, we have

$$\mathrm{ord}_2\left(\frac{p-1}{2d}\right)=\mathrm{ord}_2\left[\mathbb{F}_p^*:\langle\bar\zeta\rangle\right]\leqslant\mathrm{ord}_2\left[k^*:\langle\bar\zeta\rangle\right],\tag{7}$$

where the last inequality is an equality if and only if $[k:\mathbb{F}_p]$ is odd, equivalently $d=1$ and $[k_F:\mathbb{F}_p]$ is odd. Also,

$$\mathrm{ord}_2\left(\frac{[F':F]}{d}\right)\leqslant\mathrm{ord}_2\left(\frac{p-1}{d}\right)=\mathrm{ord}_2\left(\frac{p-1}{2d}\right)+1,\tag{8}$$

the first equality holding if and only if $(p-1)/[F':F]$ is odd. On the other hand,

$$\langle\zeta\rangle\not\subset N_{F'/F^u}F'^* \quad\Longleftrightarrow\quad \mathrm{ord}_2\left[k^*:\langle\bar\zeta\rangle\right]<\mathrm{ord}_2\left[F':F^u\right]=\mathrm{ord}_2\left(\frac{[F':F]}{d}\right).$$

If both the conditions (1) and (2) in the lemma fail, then $(p-1)/[F':F]$ is odd, F'/F is totally ramified (so $d=1$), and the inequalities in (7), (8) become equalities. Hence $\langle\zeta\rangle\not\subset N_{F'/F^u}F'^*$ and $(-1,F'/F)\neq 1$.

Conversely, if one of (1) and (2) is satisfied, one of the inequalities in (7), (8) is strict, so $\mathrm{ord}_2[k^*:\langle\bar\zeta\rangle]\geqslant\mathrm{ord}_2[F':F^u]$. In other words, ζ is norm from F' and $(-1,F'/F)=1$. □

6. p-Isogenies on formal groups

Let F be a finite extension of $\mathbb{Q}_p$ (p odd), and denote by $\mathcal{O}_F$, $\mathfrak{m}_F=(\pi_F)$, v and $k_F=\mathcal{O}_F/\mathfrak{m}_F$ its ring of integers, the maximal ideal, the valuation and the residue field respectively. Suppose E/F is an elliptic curve with semistable reduction and let $\phi:E\to E'$ be a cyclic p-isogeny defined over F. Let $f:\mathcal{F}_E(\mathfrak{m}_F)\to\mathcal{F}_{E'}(\mathfrak{m}_F)$ be the induced map on the formal groups, which can be considered as a power series of the form

$$f(T)=\alpha T+\cdots.$$

Write $|\alpha|_v=p^{-[k_F:\mathbb{F}_p]v(\alpha)}$ for the normalized absolute value of α in F and let $2^e\|p-1$. We claim that $|\alpha|_v$ is an odd power of p if and only if 2^e divides the ramification index of F_ϕ/F and $[k_F:\mathbb{F}_p]$ is odd. By Lemma 12, this will complete the proof of Theorem 6.

First of all, if $[k_F:\mathbb{F}_p]$ is even then clearly $|\alpha|_v$ is an even power of p and the statement holds. So suppose now that $[k_F:\mathbb{F}_p]$ is odd, in which case $\mathrm{ord}_p|\alpha|_v\equiv v(\alpha)\bmod 2$.

Let $\bar f:\overline{\mathcal{F}_E}\to\overline{\mathcal{F}_{E'}}$ be the reduction of f modulo $\mathfrak{m}_F$. The reduced formal groups $\overline{\mathcal{F}_E},\overline{\mathcal{F}_{E'}}$ either are those of the reduced elliptic curve in the case of good reduction, or become isomorphic to $\mathbb{G}_m$ over F^{nr} in the case of multiplicative reduction (as follows from the theory of the Tate curve, cf. [10, p. 277]). The map $\bar f$ is an isogeny of formal groups over k_F of degree dividing p, and it either has height 0 or 1 (see [13, Thm. IV.7.4]). We have two cases to consider:

Lemma 13. *If α is a unit, then F_ϕ/F is unramified.*

Proof. That α is a unit means that $\bar{f}$ is an isomorphism of the reduced formal groups. Then the group scheme $\ker\phi$ is étale over $\mathcal{O}_F$, so F_ϕ/F is unramified. $\square$

In the case that $v(\alpha) > 0$, the reduction $\bar{f}$ is an inseparable isogeny of degree p. Then we have

Lemma 14. *If $\bar{f}$ is inseparable of degree p, then f has a kernel of order p in the maximal unramified extension F^{nr} if and only if $v(\alpha)$ is a multiple of $p-1$.*

Proof. Let $\omega(T), \omega'(T)$ be the normalized invariant differentials on $\mathcal{F}_E, \mathcal{F}_{E'}$. Then [13, Cor. IV.4.3]

$$\omega' \circ f = \alpha\omega,$$

so $\alpha\omega(T) = (1 + \cdots)\frac{d}{dT} f(T)$. Because $(1 + \cdots)$ is invertible, it follows that

$$f(T) = \alpha f_1(T) + f_2\bigl(T^p\bigr)$$

for some $f_1, f_2 \in \mathcal{O}_F[[T]]$. (This is the same argument as in [13, Cor. IV.4.4].) Moreover $\bar{f}$ has height 1, so

$$f_1(T) = T + \cdots, \qquad f_2(T) = uT + \cdots \quad \bigl(u \in \mathcal{O}_F^*\bigr).$$

Now we can prove the lemma.

$\Rightarrow$ We have a kernel of order p, so $f(m) = 0$ for some $m \in \mathfrak{m}_{F^{nr}}$, $m \neq 0$. The first terms in the expansions for $f_1(m)$ and $f_2(m^p)$ must cancel modulo $\mathfrak{m}_{F^{nr}}$. Hence $v(\alpha m) = v(um^p)$, so $v(\alpha)$ is divisible by $p-1$.

$\Leftarrow$ If α has valuation divisible by $p-1$, write $\alpha = \alpha_0^{p-1}$ with $\alpha_0 \in \mathfrak{m}_{F^{nr}}$. Replace T by $T\alpha_0$, so

$$f(\alpha_0 T) = (\alpha_0)^{p-1} f_1(\alpha_0 T) + f_2\bigl((\alpha_0 T)^p\bigr) = \alpha_0^p\bigl(T + \cdots + uT^p + \cdots\bigr) = \alpha_0^p g(T),$$

with every coefficient in $\ldots$ having positive valuation. Because $g'(T)$ is a unit, by Hensel's lemma the p distinct roots of $g(T)$ mod $\mathfrak{m}_{F^{nr}}$ lift to roots z_i of $g(T)$. Then $z_i\alpha_0$ are p distinct roots of $f(T)$, so f has a kernel of order p. $\square$

Now we can complete the proof of Theorem 6. Because ϕ has p points in the kernel over F_ϕ, by the above lemmas $2^e | v_{F_\phi}(\alpha)$. If $v(\alpha)$ is odd, this means that the ramification degree of F_ϕ/F is a multiple of 2^e, as asserted. If $v(\alpha)$ is even, then over $F^{nr}(\sqrt[\frac{p-1}{2}]{\pi_F})$ the map f acquires a kernel (Lemma 14 again), so $F_\phi \subset F^{nr}(\sqrt[\frac{p-1}{2}]{\pi_F})$ has ramification degree over F not divisible by 2^e.

7. Parity conjecture for curves with a 2-isogeny

The purpose of this section is to prove Theorem 4. First note that $a \neq 0$, for otherwise $j(E) = 1728$ and E has either additive or supersingular reduction at places above 2.

Henceforth we work in the local setting. Let $F = \mathbb{R}$ or $\mathbb{C}$, or $[F : \mathbb{Q}_l] < \infty$. In the non-Archimedean case we write $\mathfrak{m}_F$ for the maximal ideal and v for the normalized valuation on F. Suppose $E, E'/F$ are elliptic curves given by Eqs. (1) and (2) with $a, b \in \mathcal{O}_F$ and $a \neq 0$. Let $\phi : E \to E'$ be the 2-isogeny with kernel $\mathcal{O}$, $(0, 0)$ and defined by (3). The discriminant

$$\Delta(E) = 16\delta b^2$$

is non-zero, so b and δ are non-zero as well. In particular, the Hilbert symbols (a, b) and $(-2a, \delta)$ make sense, and we need to prove that

$$w(E/F) = \sigma_\phi(E/F)(a, -b)(-2a, \delta).$$

7.1. *Infinite places*

First suppose that $F = \mathbb{R}$ or $\mathbb{C}$, so $w(E/F) = -1$, and $\sigma_\phi(E/F) = 1$ if and only if $\mathrm{ord}_2(\#\ker\phi/\#\operatorname{coker}\phi)$ is even. Clearly we need to show that

$$(a, -b)(-2a, \delta) = 1 \quad \Longleftrightarrow \quad \phi : E(F) \to E'(F) \text{ surjective.}$$

If $F = \mathbb{C}$, then the Hilbert symbols are trivial and ϕ is surjective.

Suppose $F = \mathbb{R}$. If $(-2a)^2 - 4\delta = 16b < 0$, then $E'(\mathbb{R}) \cong S^1$, so ϕ is always surjective. On the other hand $-b > 0$ implies $(a, -b) = 1$, and $\delta = a^2 - 4b > 0$ implies $(-2a, \delta) = 1$.

Similarly, if $b > 0$ and $\delta < 0$ then $E(\mathbb{R}) \cong S^1$ and $E'(\mathbb{R}) \cong S^1 \times \mathbb{Z}/2\mathbb{Z}$, so ϕ is not surjective; here exactly one of the Hilbert symbols is 1, depending on the sign of a.

Finally, if $b, \delta > 0$, then $E(\mathbb{R}) \cong S^1 \times \mathbb{Z}/2\mathbb{Z} \cong E'(\mathbb{R})$ and $(-2a, \delta) = 1$. Here ϕ is surjective if and only if the points $\mathcal{O}$, $(0, 0)$ of $\ker\phi$ lie on the same connected component. (If they are on different components, the image of ϕ is connected; otherwise, the identity component of $E(\mathbb{R})$ maps 2-to-1 to the identity component of $E'(\mathbb{R})$, so the other component maps to the other component since $\deg\phi = 2$.) So ϕ is surjective if and only if 0 is the rightmost root of $x^3 + ax^2 + bx$. This is equivalent to $-a < 0$ and hence to $(a, -b) = 1$.

7.2. *Finite places*

From now suppose that F is a finite extension of $\mathbb{Q}_l$. The only transformations that preserve the chosen model for E are $(x, y) \mapsto (u^4x, u^6y)$. The constituents in the Hilbert symbols then get multiplied by squares (u^2, u^4), and the Hilbert symbols are unchanged. So for $l \neq 2$ (including $l = 3$) the model (1) may and will be chosen to be minimal for the proof.

To prove the theorem, we will proceed as in the proof of Theorem 6. Recall that $\sigma_\phi(E/F) = \pm 1$ and it is 1 if and only if the power of 2 in

$$\frac{\#\operatorname{coker}(\phi : E(F) \to E'(F))}{\#\ker(\phi : E(F) \to E'(F))}$$

is even. The quotient equals $\frac{c(E')}{c(E)} \cdot |\alpha|_F^{-1}$ [1, App., formula (18)] where c is the Tamagawa number, α is the leading coefficient for the action of ϕ on the formal groups, and $|\cdot|_F$ is the normalized absolute value. We will compute $c(E)$, $c(E')$, $w(E/F)$ and $|\alpha|_F$. For the latter, $\phi^*(dx/y) = dx/y$ from the explicit formula (3) for ϕ. So if E, E' are transformed to their respective minimal models by standard substitutions $(x, y) \to (w^2x + \cdots, w^3y + \cdots)$ and $(x, y) \to (u^2x + \cdots, u^3y + \cdots)$, then $\alpha = uw^{-1}$. We distinguish between various possibilities for the reduction types.

7.3. Good reduction, $l \neq 2$

Here $w(E/F) = 1$, $\sigma_\phi(E/F) = 1$ and $b, \delta \in \mathcal{O}_F^*$. If $a \in \mathcal{O}_F^*$, then both the Hilbert symbols are (unit, unit), hence trivial. For $a \equiv 0 \bmod \mathfrak{m}_F$, the expression $-b\delta \equiv 4b^2 \bmod \mathfrak{m}_F$ is a non-zero square mod $\mathfrak{m}_F$, so the product of the Hilbert symbols is again trivial.

7.4. Additive reduction, $l \neq 2$

Reduction is either potentially multiplicative or potentially good. In the latter case, $E/F(E[4])$ has good reduction and $F(E[4])/F$ is a 2-extension, so $3|v(\Delta)$. We have the following options (writing n^+ for an integer $\geqslant n$):

Reduction	III	III*	I_0^*	I_n^* $(n > 0)$
$w(E/F)$	$(-2, \pi)$	$(-2, \pi)$	$(-1, \pi)$	$(-1, \pi)$
$v(\Delta_E)$	3	9	6	$6 + n$
$v(a), v(b), v(\delta)$	$1^+, 1, 1$	$2^+, 3, 3$	$1^+, 2, 2$	$1, 2, 3^+$ or $1, 3^+, 2$

Here π is a uniformizer of F, the reduction types are from [14, IV.9] and the root numbers are from [3,9]. Note also that E has potentially multiplicative reduction (i.e. I_n^*) if and only if E' has; the same holds for I_0^* (inertia of order 2). In what follows we continue referring to the description of Tate's algorithm in [14, IV.9] for the description of the Tamagawa numbers.

(III) Here $c(E) = c(E') = 2$. Next, $\delta \equiv -4b \bmod \pi^2$, so

$$(a, -b)(-2a, \delta) = (a, -b\delta)(-2, \delta) = \bigl(a, 4b^2 + O\bigl(\pi^3\bigr)\bigr)(-2, \pi) = (-2, \pi).$$

(III*) Same argument, replacing π^2 and $O(\pi^3)$ by π^4 and $O(\pi^5)$ respectively.

(I_0^*) By assumption, $T^3 + \frac{a}{\pi}T^2 + \frac{b}{\pi^2}T$ has 3 distinct roots mod $\mathfrak{m}_F$ over the algebraic closure, and $b = \pi^2 u$, $\delta = \pi^2 w$ with u, w units. Moreover w is a square if and only if all three roots are defined over the residue field of F, equivalently $c(E) = 4$ (otherwise $c(E) = 2$). Similarly, $c(E') = 4$ if and only if u is a square, and 2 otherwise. So

$$\begin{aligned} \operatorname{ord}_2 c(E) \equiv 0 \bmod 2 \quad &\Longleftrightarrow \quad w \in \bigl(K^*\bigr)^2 \quad \Longleftrightarrow \quad (\pi, \delta) = 1, \\ \operatorname{ord}_2 c(E') \equiv 0 \bmod 2 \quad &\Longleftrightarrow \quad u \in \bigl(K^*\bigr)^2 \quad \Longleftrightarrow \quad (\pi, b) = 1. \end{aligned} \tag{9}$$

Now,

$$(a, -b)(-2a, \delta) = (a, -b)\bigl(-2, \pi^2 w\bigr)(a, \delta) = (a, -b\delta) = (\pi, -b\delta). \tag{10}$$

The last equality is clear if $v(a)$ is odd; for $v(a) \geqslant 2$ even, $(a, -b\delta) = 1$ and

$$-b\delta = -b\bigl(a^2 - 4b\bigr) \equiv 4b^2 \mod \pi^5$$

is a square, so the last Hilbert symbol is 1 as well. Combining (9), (10) with $w(E/F) = (\pi, -1)$ yields the result.

(I_n^*) We have $v(a) = 1, v(b) \geqslant 2$ and so $v(\delta) \geqslant 2$. Because $v(\Delta) = v(b^2\delta) > 6$, one of $v(b), v(\delta)$ is at least 3, hence the other one is 2, as $\delta + 4b = a^2$; so we have essentially two cases. Swapping E and E' interchanges b and δ up to units, so E and E' will always be in two different cases. We begin by determining $c(E) \in \{2, 4\}$.

Suppose $v(b) > 2$ and $v(\delta) = 2$, so E has type I_{2n}^* with $n = v(b) - 2$. Following [14, IV.9, Step 7], the reduction of the polynomial $P(T) = T^3 + \frac{a}{\pi}T^2 + \frac{b}{\pi^2}T \bmod \mathfrak{m}_F$ has a double root at the origin; furthermore, $\frac{a}{\pi}X^2 + \frac{b}{\pi^{2+n}}X$ has two distinct roots $\bmod \mathfrak{m}_F$, so $c(E) = 4$.

Suppose $v(b) = 2$ and $v(\delta) > 2$, so E has type I_n^* with $n = v(\delta) - 2$. Translate x by $a/2$ to get a model

$$y^2 = \left(x - \frac{a}{2}\right)\left(x^2 - \frac{\delta}{4}\right),$$

so that $P(T) = (T - \frac{a}{2\pi})(T^2 - \frac{\delta}{4\pi^2})$ again has a double root at the origin $\bmod \mathfrak{m}_F$. Now, by the criterion in [14, IV.9, Step 7], we have $c(E) = 4 \Leftrightarrow \delta = \square$ for n even, and $c(E) = 4 \Leftrightarrow \frac{a}{2}\delta = \square$ for n odd.

We are now in position to compute the Hilbert symbols and to complete the proof in the I_n^* case. To simplify the argument slightly, note that showing (4) for E is equivalent to that for E': the products of the Hilbert symbols differ by $(-1, -2) = 1$, both root numbers are $(\pi, -1)$ and $\mathrm{ord}_2(c(E)/c(E')) \equiv \mathrm{ord}_2(c(E')/c(E)) \bmod 2$. So we may assume without loss of generality that $v(b) < v(\delta)$, thus $c(E') = 4$. Note that in this case

$$b = a^2 - 4\delta = a^2\bigl(1 - O(\pi)\bigr) = \square.$$

If $v(\delta)$ is even, then the parity of $\mathrm{ord}_2(c(E)/c(E'))$ is determined by the Hilbert symbol (π, δ), and

$$(a, -b)(-2a, \delta) = (a, -1)(-2, \delta)(a, \delta) = (\pi, -1)(\pi, \delta).$$

Similarly, if $v(\delta)$ is odd, then the parity of $\mathrm{ord}_2(c(E)/c(E'))$ is determined by the Hilbert symbol $(\pi, 2a\delta)$, and

$$(a, -b)(-2a, \delta) = (a, -1)(-2a, 2a\delta) = (\pi, -1)(\pi, 2a\delta).$$

7.5. A lemma on Hilbert symbols

Lemma 15. *Let $F/\mathbb{Q}_p$ be a finite extension. Then*

(1) $(1 + 4x, y) = 1$ *if* $v(x) > 0$ *and* $y \in F^*$,
(2) $(1 + 4x, y) = 1$ *if* $p = 2$, $v(x) = 0$ *and* $y \in \mathcal{O}_F^*$,
(3) $(-1, -2) = -1$ *if and only if* $p = 2$ *and* $[F : \mathbb{Q}_2]$ *is odd.*

Proof. These statements are clear for odd p, so suppose that $p=2$.

(1) See [14, Chapter V, Lemma 5.3.1].

(2) It suffices to show that the extension $F(\sqrt{1+4x})/F$ is unramified, so every unit y is a norm. Equivalently, if L/F is the unique quadratic unramified extension, we claim that $1+4x \in (L^*)^2$. Let $\bar{x} \in \mathbb{F}_{2^n}$ be the reduction of x mod $\mathfrak{m}_F$. Because every quadratic polynomial over $\mathbb{F}_{2^n}$ has a root in $\mathbb{F}_{2^{2n}}$, there is a unit z of L with $z^2+z \equiv x \bmod \mathfrak{m}_F$. Then

$$(1+2z)^2 = 1+4\big(z+z^2\big) \equiv 1+4x \mod 4\mathfrak{m}_F,$$

so $(1+4x)/(1+2z)^2$ is a square in L by part (1), and so is $1+4x$.

(3) If $\sqrt{-2} \in F$, then both of the conditions hold. Otherwise,

$$\begin{aligned}(-1,-2)_K &= \big(-1, F\big(\sqrt{-2}\big)/F\big) = \big(N_{F/\mathbb{Q}_2}(-1), \mathbb{Q}_2\big(\sqrt{-2}\big)/\mathbb{Q}_2\big)\\ &= \big((-1,-2)_{\mathbb{Q}_2}\big)^{[F:\mathbb{Q}_2]} = (-1)^{[F:\mathbb{Q}_2]},\end{aligned}$$

as asserted. □

7.6. *Good reduction, $l=2$, 2-torsion point reduces to $\bar{P} = \mathcal{O}$*

Suppose $l=2$ and E/F has good reduction, so $w(E/F)=1$ and $c(E)=c(E')=1$. By assumption, the reduction is ordinary, equivalently $j(E)$ is a unit. By [13, A.1.1c], we can choose a minimal model of E over $\mathcal{O}_F$ of the form

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6, \quad 1-a_1, a_3, a_4 \in \mathfrak{m}_F.$$

After the substitution $(x,y) \mapsto (a_1^2x - a_3a_1^{-1}, a_1^3y)$, we may assume $a_1=1$ and $a_3=0$. Next, the substitution $(x,y) \mapsto (x-2t, y+t)$ with $t \in \mathfrak{m}_F$ a root of $12t^2-(1+4a_2)t+a_4=0$ (Hensel's lemma) eliminates a_4. Neither substitution changes the reduced curve, thus we may assume that our model is

$$y^2+xy = x^3+a_2x^2+a_6, \quad a_2 \in \mathcal{O}_F,\ a_6 \in \mathcal{O}_F^*.$$

After completing the square, this becomes

$$y^2 = x^3+\left(a_2+\frac{1}{4}\right)x^2+a_6.$$

Now let $(x_0, 0)$ be our 2-torsion point with $v(x_0)<0$. Then

$$x_0^2\left(x_0+a_2+\frac{1}{4}\right) = -a_6 \in \mathcal{O}_F^*,$$

so $v(x_0+a_2+1/4) = -2v(x_0) > 0$, hence $v(x_0) = -v(4)$. Then $v(x_0+a_2+1/4) = v(16)$, and write $x_0+a_2+1/4 = 16v$ with v a unit. Letting $w = 1+4a_2$ and translating x by x_0, the curve becomes

$$y^2 = x^3+ax^2+bx,$$

with

$$a = \frac{1}{2}(-w + 96v) = -\frac{w}{2} \cdot \Box,$$
$$b = \frac{1}{16}(-w + 64v)(-w + 192v) = \Box,$$
$$\delta = a^2 - 4b = -16v(-w + 48w) = vw \cdot \Box.$$

Therefore

$$(a, -b)(-2a, \delta) = \left(-\frac{w}{2}, -1\right)(w, vw) = (-2, -1)(w, -vw) = (-2, -1),$$

where the last equality holds since (1 mod 4, unit) = 1. On the other hand, the isogenous curve

$$E' : y^2 = x^3 - 2ax^2 + \delta x$$

transforms under $x \to 4x$, $y \to 4x + 8y$ to

$$y^2 + xy = x^3 + (a_2 - 24v)x^2 + (4a_2 - 48v + 1)x,$$

which has good reduction at 2. So $\mathrm{ord}_2 |\alpha|_F = \mathrm{ord}_2 |2|_F$ is even if and only $[F : \mathbb{Q}_2]$ is even if and only if $(-2, -1) = 1$ (Lemma 15).

7.7. Good reduction, $l = 2$, 2-torsion point reduces to $\bar{P} \neq \mathcal{O}$

As before, $w(E/F) = 1$ and $c(E) = c(E') = 1$. We claim that $\alpha = 1$, and that both Hilbert symbols are trivial. Translating the 2-torsion point on the reduction to $(0, 0)$, we get a model

$$E: \quad y^2 + xy = x^3 + a_2x^2 + a_4x, \quad a_2 \in \mathcal{O}_F, a_4 \in \mathcal{O}_F^*,$$
$$E': \quad y^2 + xy = x^3 + a_2x^2 - 4a_4x - (4a_2 + 1)a_4.$$

These transform to our models (1), (2) with substitutions $x \to x + \cdots$, $y \to y + \cdots$, so $\alpha = 1$. Next (cf. Lemma 15, part (2)),

$$a = a_2 + 1/4,$$
$$b = a_4,$$
$$\delta = (a_2 + 1/4)^2 - 4a_4 = 1/16 + a_2/2 + a_2^2 - 4a_4,$$
$$(a, -b) = (a_2 + 1/4, -a_4) = (1 + 4a_2, -a_4) = (1 \bmod 4, \mathrm{unit}) = 1,$$
$$(-2a, \delta) = \left(-2a, 1 + 8a_2 + 16a_2^2 - 64a_4\right) = (-2a, \Box) = 1.$$

7.8. Split multiplicative primes

Write E as a Tate curve [14, §V.3]

$$E_q: y^2 + xy = x^3 + a_4(q)x + a_6(q), \qquad E(F) \cong F^*/q^{\mathbb{Z}},$$

with $q \in m_K$ of valuation $v(q) = v(\Delta)$. The coefficients have expansions

$$a_4(q) = -5s_3(q), \qquad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}, \quad s_k(q) = \sum_{n\geqslant 1} \frac{n^k q^n}{1-q^n},$$

and they start

$$a_4(q) = -5q - 45q^2 - 140q^3 - 365q^4 - 630q^5 + O(q^6),$$
$$a_6(q) = -q - 23q^2 - 154q^3 - 647q^4 - 1876q^5 + O(q^6).$$

The two-torsion, as a Galois set, is $\{1, -1, \sqrt{q}, -\sqrt{q}\}$. For $u \neq 1$ in this set, the corresponding point on E has coordinates

$$X(u,q) = \frac{u}{(1-u)^2} + \sum_{n\geqslant 1}\left(\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}\right),$$
$$Y(u,q) = \frac{u^2}{(1-u)^3} + \sum_{n\geqslant 1}\left(\frac{q^{2n} u^2}{(1-q^n u)^3} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} + \frac{q^n}{(1-q^n)^2}\right).$$

We now have two cases to consider: the 2-torsion point $(X(-1,q), Y(-1,q)) \in E_q$ and (renaming $\pm\sqrt{q}$ by q) the 2-torsion point $(X(q,q^2), Y(q,q^2)) \in E_{q^2}$. In both cases, we have $c(E)/c(E') = 2^{\pm 1}$ and $w(E/F) = -1$, so we need

$$\operatorname{ord}_2 |\alpha|_F \text{ even} \quad \Longleftrightarrow \quad (a, -b)(-2a, \delta) = 1, \tag{11}$$

where a, b, δ are the invariants of the curve (1), when our curve is transformed into that from with the 2-torsion point at $(0,0)$. First of all, E_q has a model

$$y^2 = x^3 + x^2/4 + a_4(q)x + a_6(q).$$

Let $r = -X(u,q)$, and write $a_4 = a_4(q), a_6 = a_6(q)$. Then, after translation, the curve becomes

$$E: y^2 = x^3 + ax^2 + bx, \quad a = 1/4 - 3r, \ b = 2a_4 - r/2 + 3r^2.$$

Recall that the isogenous curve E' is (2) in this form.

Suppose we are in Case 1, so $r = -X(-1,q)$. Then the substitution

$$x \to 4x - 2r + 1/2, \qquad y \to 8y + 4x \tag{12}$$

transforms E' into the form

$$E^\dagger : y^2 + xy = x^3 + \bigl(-5q^2 + O\bigl(q^4\bigr)\bigr)x + \bigl(-q^2 + O\bigl(q^4\bigr)\bigr).$$

We use the notation $O(q^n)$ to indicate a power series in q with coefficients in $\mathcal{O}_F$ that begins with $a_n q^n + \cdots$. In fact, $E^\dagger = E_{q^2}$ but we will not need this; it is only important that it is again a Tate curve (in particular, this model is minimal), and $\alpha = 2$ (this comes from (12)). So

$$\mathrm{ord}_2 |\alpha|_F \text{ even} \iff l \neq 2 \quad \text{or} \quad [F : \mathbb{Q}_2] \text{ is even} \iff (-1, -2) = 1.$$

Finally, from the expansions

$$r = 1/4 + 4O(q), \quad a = -1/2 + 4O(q), \quad b = 1/16 + O(q),$$

we have

$$\begin{aligned}
(a, -b) &= (a, -1)(a, b) = (a, -1)(a, \square) = \bigl(-1/2 + 4O(q), -1\bigr) \\
&= (-1/2, -1)\bigl(1 + 8O(q), -1\bigr) = (-2, -1)(\square, -1) = (-1, -2), \\
(-2a, \delta) &= \bigl(1 - 8O(q), \delta\bigr) = (\square, \delta) = 1.
\end{aligned}$$

Case 2 is similar and we omit the details; here α is a unit, so we need to show that the product of the two Hilbert symbols is 1. Here

$$a = 1/4 + 2\,O(q), \qquad b = q + O\bigl(q^2\bigr), \qquad \delta = 1/16 + O(q).$$

In particular, a and δ are squares in F, so both Hilbert symbols are trivial.

7.9. Non-split multiplicative primes

Let $F(\eta)/F$ be the quadratic unramified extension of F and consider the twist of E by η,

$$\begin{aligned}
E&: \quad y^2 = x^3 + ax^2 + bx, \\
E_\eta&: \quad y^2 = x^3 + \eta a x^2 + \eta^2 b x.
\end{aligned}$$

Then E_η has split multiplicative reduction, so (cf. (11))

$$\mathrm{ord}_2 |\alpha_{E_\eta}|_F \text{ even} \quad \iff \quad \bigl(\eta a, -\eta^2 b\bigr)\bigl(2\eta a, \eta^2\bigl(a^2 - 4b\bigr)\bigr) = 1.$$

Also $\alpha_{E_\eta} = \alpha_E$, since the two curves become isomorphic over K_η. Now,

$$\begin{aligned}
&\bigl(\eta a, -\eta^2 b\bigr) = (\eta a, -b) = (\eta, -b)(a, -b), \\
&\bigl(2\eta a, \eta^2\bigl(a^2 - 4b\bigr)\bigr) = \bigl(2\eta a, a^2 - 4b\bigr) = \bigl(\eta, a^2 - 4b\bigr)\bigl(2a, a^2 - 4b\bigr),
\end{aligned}$$

so comparing with the Hilbert symbols in (4) we have an extra term

$$\bigl(\eta, -b\bigl(a^2 - 4b\bigr)\bigr) = \bigl(\eta, -b^2\Delta(E')/16\Delta(E)\bigr) = \bigl(\eta, -\Delta(E')/\Delta(E)\bigr). \tag{13}$$

Because x is a norm from $F(\eta)^*$ to F^* if and only if $v(x)$ is even, this Hilbert symbol is trivial precisely when $v(\Delta(E')) \equiv v(\Delta(E)) \bmod 2$. From Tate's algorithm [14, IV.9.4, Step 2],

$$c(E) = \begin{cases} 1, & v(\Delta(E)) \text{ odd}, \\ 2, & v(\Delta(E)) \text{ even}, \end{cases} \qquad c(E') = \begin{cases} 1, & v(\Delta(E')) \text{ odd}, \\ 2, & v(\Delta(E')) \text{ even}, \end{cases}$$

so the correction term (13) is trivial if and only $c(E)/c(E')$ has even 2-valuation. This proves (4) in the non-split multiplicative case.

Acknowledgments

We would like to thank the referee for carefully reading the manuscript and numerous comments and suggestions.

References

[1] V. Dokchitser, Root numbers of non-abelian twists of elliptic curves (with an appendix by T. Fisher), Proc. London Math. Soc. (3) 91 (2005) 300–324.
[2] A. Fröhlich, J. Queyrut, On the functional equation of the Artin L-function for characters of real representations, Invent. Math. 20 (1973) 125–138.
[3] S. Kobayashi, The local root number of elliptic curves with wild ramification, Math. Ann. 323 (2002) 609–623.
[4] K. Kramer, J. Tunnell, Elliptic curves and local ϵ-factors, Compos. Math. 46 (1982) 307–352.
[5] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, Manuscripta Math. 69 (4) (1990) 353–385.
[6] P. Monsky, Generalizing the Birch–Stephens theorem. I: Modular curves, Math. Z. 221 (1996) 415–420.
[7] J. Nekovář, Selmer complexes, Astérisque, in press.
[8] D. Rohrlich, Elliptic curves and the Weil–Deligne group, in: Elliptic Curves and Related Topics, in: CRM Proc. Lecture Notes, vol. 4, Amer. Math. Soc., Providence, RI, 1994, pp. 125–157.
[9] D. Rohrlich, Galois theory, elliptic curves, and root numbers, Compos. Math. 100 (1996) 311–349.
[10] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331.
[11] J.-P. Serre, J. Tate, Good reduction of abelian varieties, Ann. of Math. 68 (1968) 492–517.
[12] M. Shuter, paper in preparation.
[13] J.H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts Math., vol. 106, Springer-Verlag, 1986.
[14] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Grad. Texts Math., vol. 151, Springer-Verlag, 1994.
[15] J. Tate, Number theoretic background, in: Proc. Sympos. Pure Math., vol. 33, Part 2, 1979, pp. 3–26.